



Patent

Attorney's Docket No. 1033048-000019

Handwritten initials: ZW, AX

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of)	MAIL STOP APPEAL BRIEF-
Paul Kennedy)	PATENTS
Application No.: 09/841,008)	Group Art Unit: 2131
Filed: April 25, 2001)	Examiner: CHRISTIAN A
For: ACCESS AUTHENTICATION FOR)	LAFORGIA
DISTRIBUTED NETWORKS)	Confirmation No.: 4932
)	
)	
)	

RESPONSE TO NOTIFICATION OF NON-COMPLIANT APPEAL BREIF

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

In response to the Notification dated August 15, 2006, submitted herewith is a substitute Appeal Brief containing a Summary in which each of the independent claims is individually mapped to the disclosure.

Respectfully submitted,

BUCHANAN INGERSOLL & ROONEY, P.C.

Date: September 15, 2006

By: *James A. LaBarre*
James A. LaBarre
Registration No. 28,632

P.O. Box 1404
Alexandria, Virginia 22313-1404
(703) 836-6620



Attorney's Docket No. 1033048-000019

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of)

Paul Kennedy)

Application No.: 09/841,008)

Filed: April 25, 2001)

For: ACCESS AUTHENTICATION
FOR DISTRIBUTED NETWORKS)

Group Art Unit: 2131

Examiner: CHRISTIAN A
LAFORGIA

Appeal No.: _____

APPEAL BRIEF

Mail Stop APPEAL BRIEF - PATENTS

Commissioner for Patents

P.O. Box 1450

Alexandria, VA 22313-1450

Sir:

This appeal is from the decision of the Primary Examiner dated October 7, 2005, finally rejecting claims 9-25, which are reproduced as the Claims Appendix of this brief.

The requisite fee under 37 C.F.R. § 41.20 (b)(2) was previously submitted with the original Appeal Brief filed June 7, 2006,



Table of Contents

	Page
I. Real Party in Interest.....	1
II. Related Appeals and Interferences.....	1
III. Status of Claims.....	1
IV. Status of Amendments.....	1
V. Summary of Claimed Subject Matter.....	1
VI. Grounds of Rejection to be Reviewed on Appeal.....	3
VII. Argument	4
VIII. Claims Appendix	7
IX. Evidence Appendix	7
X. Related Proceedings Appendix.....	7



I. Real Party in Interest

The subject application is assigned to Opware, Inc., the successor in interest to LoudCloud, Inc.

II. Related Appeals and Interferences

There are no other prior or pending appeals, interferences, or judicial proceedings which may be related to, directly affect or be directly affected by, or have a bearing on the Board's decision in this appeal.

III. Status of Claims

The application contains claims 1-25. Claims 1-8 have been canceled. Claims 9-25 are pending and stand finally rejected, and form the basis for this appeal.

IV. Status of Amendments

There were no amendments filed subsequent to the final Office Action.

V. Summary of Claimed Subject Matter

The appealed claims comprise three independent claims, namely claims 9, 16 and 21. Claim 9 recites a method for authenticating users to individual network devices that are distributed among a plurality of locations. The first step of the method comprises storing a directory structure at one of the locations (Figure 1, directory structure 102; page 8, lines 9-10). The directory structure comprising a root node (Figure 2, master node 202; page 11, lines 24-25), a first level of nodes below the root node that are associated with respective organizations to which the network devices are assigned (Figure 2, customer level containing nodes 204, 206, 208; page 11-lines 25-27), and at least one further level of nodes below the first level that identify users who are authorized to access the network devices assigned to the organization associated with a parent first-level node and authentication information for the users (Figure 2, "People" node; page 12, lines 3-8). The second step of the claim comprises replicating the directory structure among the plurality of locations

(page 8, lines 14-27; Figure 1, directory structures 114-124). The claim further recites that, in response to a request by a user for access to one of the network devices, determining which organization to which the one device is assigned and whether the user is identified on a node below the first-level node associated with the determined organization (page 13, lines 20-26). As a final step, the claim recites authenticating the user to the device if the user is so identified (page 14, lines 11-14).

Claim 16 recites a data center comprising a plurality of network resources (Figure 1, data centers 108-112; page 7, lines 3-4) and a directory server for authenticating users for access to the network resources by means of a directory structure (Figure 1, directory structures 114-124; page 8, lines 18-21). The directory structure comprises a root node (Figure 2, master node 202; page 11, lines 24-25), a first level of nodes below the root node that are associated with respective organizations to which the network resources are assigned (Figure 2, customer level containing nodes 204, 206, 208; page 11-lines 25-27), and at least one further level of nodes below the first level that identify users who are authorized to access the network resources assigned to the organization associated with a parent first-level node and authentication information for the users (Figure 2, "People" node; page 12, lines 3-8).

Claim 21 recites a distributed network having network resources distributed among a plurality of locations, and comprising a master directory server at one of the locations (Figure 1, master data center 104; page 8, lines 8-10). The master directory server contains a directory structure (Figure 1, directory structure 102) comprising a root node (Figure 2, master node 202; page 11, lines 24-25), a first level of nodes below the root node that are associated with respective organizations to which the network resources are assigned (Figure 2, customer level containing nodes 204, 206, 208; page 11-lines 25-27), and at least one further level of nodes below the first level that identify users who are authorized to access the network resources assigned to the organization associated with a parent first-level node and authentication information for the users (Figure 2, "People" node; page 12, lines 3-8). The claim further recites at least one directory server at each of the other locations, each of the directory servers containing a replicated copy of the directory structure

(Figure 1, data centers 108-112 and directory structures 114-124; page 8, lines 14-27).

VI. Grounds of Rejection to be Reviewed on Appeal

The final Office Action presents two grounds of rejection for review on this appeal:

1. Claims 9-12, 14-18, 20-23 and 25 stand rejected under 35 U.S.C. §103, as being unpatentable over the Aldred et al patent (US 6,438,549) in view of the Byrne et al patent (US 6,708,170); and
2. Claim 13, 19 and 24 stand rejected under 35 U.S.C. §103 as being unpatentable over the Aldred and Byrne patents, in further view of the Pang patent (US 6,446,204).

VII. Argument

A. Claims 9, 16 and 21

Independent claim 9 recites a method for authenticating users to individual network devices that are distributed among a plurality of locations. Independent claim 16 recites a data center comprising a plurality of network resources and a directory server. Independent claim 21 recites a distributed network having network resources distributed among a plurality of locations. Among other elements, each of these three claims recites a directory structure that is stored at a location within the network, and specifically in the case of claim 16, at a data center. The claims recite that the directory structure comprises a root node, a first level of nodes below the root node that are associated with respective organizations to which network resources are assigned, and at least one further level of nodes below the first level that identify users who are authorized to access the network resources assigned to the organization associated with a parent first level node, and authentication information for those users.

Each of claims 9, 16 and 21 stands finally rejected as being obvious over the Aldred patent in view of the Byrne patent. MPEP § 2143 sets forth three criteria that must be met to establish a prima facie case of obviousness. One of these criteria is that "the prior art reference (or references when combined) must teach or suggest all the claim limitations." The rejection of claims 9, 16 and 21 fails to meet at least this requirement.

In rejecting the claims, the final Office Action asserts that the above-noted subject matter recited in each of claims 9, 16 and 21 is disclosed in the Aldred patent, with specific reference to Figures 1, 2 and 7, as well as column 3, line 64 to column 4, line 20, and column 6, lines 51-60. In the cited passage at columns 3 and 4, the Aldred patent discloses the general structure of a directory tree. It does not, however, disclose a directory having the particular features recited in the claims, namely a root node, a first level of nodes below the root node associated with respective organizations, and at least one further level of nodes that identify users who are authorized to access the network devices.

Nor does it suggest the use of a directory structure as the mechanism to store information for authenticating users to network resources. Insofar as access control is concerned, the Aldred patent discloses the use of access control lists (ACLs), beginning at column 4, line 65. Referring to the disclosure beginning at column 5, line 17, as well as Figure 5, the Aldred patent discloses that the ACL information is stored in a relational database management system 39. The passage at column 6, lines 51-60, cited in the Office Action, relates to one of the tables that are stored in the relational database.

Thus, unlike the claimed subject matter, the Aldred patent does not disclose that access control information is contained at certain nodes within the directory tree itself. Rather, the patent is representative of the prior art described in the background portion of the present application, in which access control information is stored in a database. As can be seen in Figure 5, the database 39 is distinct from the directory server 37.

Since the Aldred patent does not disclose a directory structure that is arranged in the manner recited in claims 9, 16 and 21 to store access information, it also does not disclose other features recited in the claims. For example, claim 9 recites a step which is responsive to a request by a user for access to one of the network devices to determine the organization to which that device is assigned and "whether said user is identified on a node below the first-level node associated with the determined organization." In the system of the Aldred patent, access control is determined with reference to the permissions table 47 stored in the relational database. It does not determine whether a user is identified on a node at a particular level of the directory tree.

The Byrne patent was cited for its disclosure of replicating authentication information at individual servers. However, it does not overcome the above-noted differences between the claimed subject matter and the disclosure of the Aldred patent. In particular, it does not disclose the use of a directory structure to maintain authentication information associated with different organizations, in the manner recited in claims 9, 16 and 21.

Accordingly, the Aldred and Byrne patents, whether considered individually or in combination, do not teach or suggest all of the subject matter recited in the claims. For at least this reason, a prima facie case of obviousness has not been established.

B. Claims 10, 17 and 22

Claim 10 recites that the directory includes nodes below the first level that identify resources of an organization to which authenticated users are allowed access. Claims 17 and 22 recite similar subject matter.

The final Office Action asserts that this claimed subject matter is disclosed in the Aldred patent, at column 4, line 65 to column 5, line 16. However, this portion of the patent does not pertain to the information stored at certain levels of a directory. Rather, as noted previously, it deals with the Access Control Lists, which are separate from the LDAP directory. There is no teaching in the Aldred patent regarding the type of information stored of various levels within a directory. In particular, there is no teaching of storing resources in relation to an organization to which users are allowed access, as recited in the claims.

C. Claims 14, 18 and 23

These claims recite that the same user identification and authentication information is contained at a plurality of nodes respectively associated with different first-level nodes. In rejecting these claims, the final Office Action again refers to the Aldred patent at column 14, line 65 to column 5, line 16. For the reasons presented above, this portion of the patent does not support the rejection. It has nothing to do with the type of information stored in particular nodes of the directory, let alone teach that the same information is stored in plural nodes.

D. Claims 13, 19 and 24

Claim 13 depends from claim 9, and recites that at least some of locations contain at least two replicated copies of the directory structure. The claim recites the further step of distributing access requests among the replicated copies by means of a load balancer. Claims 19 and 24 also recite the concepts of having at least two

directory servers and a load balancer that distributes requests for access to resources among the directory servers.

In the rejection of claims 13, 19 and 24, the Pang patent was cited as disclosing at least two replicated copies of a directory structure, and distributing access requests among the replicated copies by means of a load balancer. While the cited passage at column 23, lines 50-64, discloses the use of a load balancing scheme to balance the workload of multiple authentication hosts, it does not disclose the use of a directory structure to store the identification of users who are authorized to access network resources, as discussed above. Hence, the Pang patent also does not overcome the distinctions between the claimed subject matter and the disclosure of the Aldred patent.

VIII. Claims Appendix

See attached Claims Appendix for a copy of the claims involved in the appeal.

IX. Evidence Appendix

(none)

X. Related Proceedings Appendix


(none)

Respectfully submitted,

Buchanan Ingersoll PC

Date September 15, 2006

By: _____


James A. LaBarre
Registration No. 28632

P.O. Box 1404
Alexandria, VA 22313-1404
703.836.6620



VIII. CLAIMS APPENDIX

The Appealed Claims

9. A method for authenticating users to individual network devices that are distributed among a plurality of locations, comprising the following steps:

storing a directory structure at one of said locations, said directory structure comprising a root node, a first level of nodes below said root node that are associated with respective organizations to which said network devices are assigned, and at least one further level of nodes below said first level that identify users who are authorized to access the network devices assigned to the organization associated with a parent first-level node and authentication information for said users;

replicating said directory structure among said plurality of locations;

in response to a request by a user for access to one of said network devices, determining which organization to which said one device is assigned and whether said user is identified on a node below the first-level node associated with the determined organization; and

authenticating said user to said device if the user is so identified.

10. The method of claim 9, wherein said directory structure further includes nodes below said first level that identify resources of an associated organization to which authenticated users are allowed access.

11. The method of claim 9, wherein said determining step is performed with reference to a replicated copy of said directory structure at the location containing said one device.

12. The method of claim 9 wherein said network devices comprise servers, and said locations are data centers.

13. The method of claim 9, wherein at least some of said locations contain at least two replicated copies of said directory structure, and further including the steps of distributing access requests among said replicated copies by means of a load balancer.

14. The method of claim 9, wherein the same user identification and authentication information is contained at a plurality of said further level nodes that are respectively associated with different ones of said first-level nodes.

15. The method of claim 9, wherein said replicating step is carried out automatically without user input.

16. A data center comprising a plurality of network resources and a directory server for authenticating users for access to said network resources by means of a directory structure comprising a root node, a first level of nodes below said root node that are associated with respective organizations to which said network resources are assigned, and at least one further level of nodes below said first level that identify users who are authorized to access the network resources assigned to the organization associated with a parent first-level node and authentication information for said users.

17. The data center of claim 16, wherein said directory structure further includes nodes below said first level that identify resources of an associated organization to which authenticated users are allowed access.

18. The data center of claim 16, wherein the same user identification and authentication information is contained at a plurality of said further level nodes that are respectively associated with different ones of said first-level nodes.

19. The data center of claim 16, comprising at least two of said directory servers, and further including a load balancer that distributes requests for access to said resources among said directory servers.

20. The data center of claim 16, wherein at least some of network resources are servers that each include an authentication module that is responsive to a request for access to determine the organization to which its corresponding server is assigned and restrict directory searches to the further-level nodes below the first-level node associated with the determined organization.

21. A distributed network having network resources distributed among a plurality of locations, and comprising:

a master directory server at one of said locations, said master directory server containing a directory structure comprising a root node, a first level of nodes below said root node that are associated with respective organizations to which said network resources are assigned, and at least one further level of nodes below said first level that identify users who are authorized to access the network resources assigned to the organization associated with a parent first-level node and authentication information for said users; and

at least one directory server at each of the other locations, each of said directory servers containing a replicated copy of said directory structure.

22. The distributed network of claim 21, wherein said directory structure further includes nodes below said first level that identify resources of an associated organization to which authenticated users are allowed access.

23. The distributed network of claim 21, wherein the same user identification and authentication information is contained at a plurality of said further level nodes that are respectively associated with different ones of said first-level nodes.

24. The distributed network of claim 21, wherein at least some of said locations contain at least two directory servers, and further including a load balancer that distributes requests for access to said resources among said directory servers.

25. The distributed network of claim 21, wherein at least some of network resources are servers that each include an authentication module that is responsive to a request for access to determine the organization to which its corresponding server is assigned and restrict directory searches to the further-level nodes below the first-level node associated with the determined organization.